UNITED STATES PATENT APPLICATION

OF

Vyacheslav S. Belenko and Vsevolod M. Kuzmich

For

COPY PROTECTION METHOD AND SYSTEM FOR DIGITAL MEDIA

CROSS-REFERECNE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 60/265,890, filed on February 5, 2001, in the name of inventors Vyacheslav S. Beleko and Vsebolod M. Kumich, titled "Cryptography Architecture for Digital Media Protection Technology", which is hereby incorporated by reference as if fully set forth herein.

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The present invention relates to media copy protection, and more particularly, to digital media copy protection method and system that prevent any unauthorized access to a digital media data set using a hybrid cryptographic technique.

Discussion of the Related Art

[0003] Communication systems such as computer networks, telecommunication systems, and other systems are increasingly using cryptography for the security of information. There are two main classes of cryptographic systems: symmetric key and public key cryptographic systems. In a symmetric key cryptographic

system, a symmetric (secrete) key is used for both of data encryption and decryption processes. There are several efficient implementations of the symmetric key cryptographic system, but the actual key managements of such implementations are often troublesome.

[0004] On the other hand, in a public key cryptographic system, the data encryption and decryption processes are independent from each other. That is, the data encryption process requires a public key, often designated as e, while the data decryption process requires a different (but mathematically related) private key d. Therefore, an entity being possessed of the public key may encrypt a plaintext, which is the original form of a message, but the entity may not be able decrypt a ciphertext, which is the encrypted form of the message.

[0005] If an entity selects a public key and publishes the public key, anyone is able to use the key to encrypt one or more messages for the entity. Then the entity keeps his private key secret so that he or she is the only one who can decrypt the ciphertexts of the messages. The implementations of the public key cryptographic systems are currently less efficient than those of the symmetric key cryptographic systems, but they are much safer.

[0006] In a hybrid cryptographic system, a plaintext is encrypted with a symmetric key corresponding to a symmetric algorithm. The symmetric key is then encrypted with a public key having a public algorithm. When a receiver receives the public key-encrypted symmetric key and the symmetric key-encrypted data, the receiver initially decrypts the symmetric key by using his own private key. Subsequently, the receiver decrypts the encrypted data by using the decrypted symmetric key. The processes of obtaining the original data in a hybrid cryptographic system are usually faster than those of the public key cryptographic system. In addition, a hybrid cryptographic system may allow using a different symmetric key each time, considerably enhancing the security of the symmetric algorithm. For that reason, the hybrid cryptographic systems are ideal for transferring the protected media data safely to a receiver.

SUMMARY OF THE INVENTION

[0007] Accordingly, the present invention is directed to a copy protection method and system for digital media data that substantially obviates one or more problems due to limitations and disadvantages of the related art.

[0008] An object of the present invention is to provide a copy protection method that prevents any unauthorized access to a

digital media data set by using a hybrid cryptographic technique and a media certificate.

[0009] Another object of the present invention is to provide a copy protection system that prevents any unauthorized access to a digital media data set by using a hybrid cryptographic technique and a media certificate.

[0010] Additional advantages, objects, and features of the invention will be set forth in part in the description which follows and in part will become apparent to those having ordinary skill in the art upon examination of the following or may be learned from practice of the invention. The objectives and other advantages of the invention may be realized and attained by the structure particularly pointed out in the written description and claims hereof as well as the appended drawings.

[0011] To achieve these objects and other advantages and in accordance with the purpose of the invention, as embodied and broadly described herein, a copy protection method for digital media includes (a) encrypting an original media data set with a media key corresponding to a symmetric algorithm and encrypting the media key with a public key of a compliant playing device; (b) delivering the media data set and media key encrypted in the step (a) and a media certificate to the playing device, the certificate including a private-key identification of the playing

device, the private-key identification being encrypted with the public key; and (c) decrypting the private-key identification.

[0012] The method further includes (d) searching for an actual private key by checking whether each of stored private keys of the playing device corresponds to the decrypted private-key identification; (e) decrypting the delivered media key with the actual private key; and (f) decrypting the delivered media data set with the decrypted media key.

[0013] In another aspect of the present invention, a copy protection system for digital media includes a private key verifier receiving a media certificate that includes a private-key identification of a compliant playing device and searching for an actual private key by checking whether each of available private keys of the playing device corresponds to the private-key identification; a media key decryptor receiving an encrypted media key and decrypting the media key with the actual private key; and a media data decryptor receiving an encrypted media data set and decrypting the media data set with the decrypted media key.

[0014] It is to be understood that both the foregoing general description and the following detailed description of the present invention are exemplary and explanatory and are intended to provide further explanation of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this application, illustrate embodiment(s) of the invention and together with the description serve to explain the principle of the invention. In the drawings;

[0016] FIG. 1 illustrates the media data decryption process according to the present invention;

[0017] FIG. 2 illustrates the process of extracting an actual private key by using a media certificate in accordance with the present invention; and

[0018] FIG. 3 illustrates the automatic key-renewing process according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0019] Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

[0020] The media protection method according to the present invention, which is shown in FIG. 1, is based on general hybrid

cryptographic principles. In a hybrid cryptographic system, a media data set is encrypted with a media (symmetric) key having a symmetric algorithm, and the media key is also encrypted. The encryption of the media key is performed independently for each compliant device's public key. Then the encrypted media data set and media key are delivered to one or more target playing devices.

[0021] When one of the playing devices plays the received media data set, the device uses its own private key to decrypt the encrypted media key. Subsequently, the device uses the decrypted media key to decrypt the encrypted media data set. These processes are shown in FIG. 1. The cryptographic levels of the public-key encryption of the media key and the media-key encryption of the media data set are chosen so that the encrypted data are safe enough to resist against any known types of attacks.

[0022] In general, different groups of devices have different private keys. The device grouping principles are out of the scope of the present invention. When a media data set is delivered to devices having different private keys, the data set must contain several different samples of the media key, one for each device's private key. Then each device must be able to recognize its own encrypted sample in order to obtain a valid media key. This can be done in a digital media format-specific manner.

[0023] In addition, each device may have several available private keys due to any key revocation processes: a current private key and several revoked private keys. A media data set currently being played by a playing device may be a new data set or an old data set that was played previously. In order to recognize a valid private key among the available keys in such case, a media certificate included in the media data set can be used.

[0024] Every media data set contains several media certificates, one for each group of devices having a same private key. A media certificate includes the media identification and the private key identification of a group of devices. The private key identification is generated by encrypting the media identification with the public key of each device. In this way, each compliant device can easily recognize its own private key by decrypting the media identification and comparing the recognized key with the original one.

[0025] A playing device must have a secure and rewritable memory storage for storing all the older private keys. All the data stored in this memory storage must be encrypted with a current public key. Before the playing device plays a media data set, it initiates an appropriate private key search process, which is shown in FIG. 2. As it is shown in the figure, all the

stored private keys including a current private key are tested with a media certificate until a "right" private key is found. If no "right" key is found, the media data set is considered as being unplayable.

[0026] For compromising a private key of a device, a key-renewing certificate can be delivered to the device together with a media data set. The storage of the key-renewing certificate on the media data set is out of the scope of the present invention. The key-renewing certificate contains a pair of new public and private keys of the device, which are encrypted with a master public key of the device. The master public key and its corresponding master private key of the device are stored inside of the device. For the security reasons, the master private key of the device must be encrypted with a current public key of the device. The certificate further contains time marks for sequencing the public and private keys from the oldest to the newest, respectively.

[0027] First, a key-renewing certificate is processed by using a device master key, and the time marks are analyzed. If the issued key-renewing certificate is the newest one, the extracted public and private keys replace the older key pair. The previous private key is included in a private key history database, and the whole database and a master private key are re-

encrypted with a new public key. This process is illustrated in FIG. 3.

[0028] A master key compromise of a device is very improbable, but it does not mean that it never happens. If it occurs by any chance, a new media data set must be issued with key-renewing certificates associated with a new master key, and any device receiving the media data set is subjected to replace its master key with the customer service.

[0029] It will be apparent to those skilled in the art that various modifications and variations can be made in the present invention without departing from the spirit or scope of the inventions. Thus, it is intended that the present invention covers the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.